Architectures for Protecting Cloud Data Planes

论文阅读

蒋隽　*2022.5.8*

Zero Trust Architecture

BACKGROUND——ZERO TRUST ARCHITECTURE

➤ 零信任安全模型的提出

S. Rose, O. Borchert, S. Mitchell, S. Connelly, “NIST Special Publication 800-207: Zero Trust Architecture”, August 2020 - https://doi.org/10.6028/NIST.SP.800-207
（NIST提出的一个零信任安全模型）

Cybersecurity and Infrastructure Security Agency, US Digital Service, and FedRAMP. “Cloud Security Technical Reference Architecture”. August 2021. https://www.cisa.gov/publication/cloud-security-technical-reference-architecture
（CISA宣布了它的云安全和中的零信任技术参考架构草案）

这些文档讨论了零信任保护的目标和市场上各种供应商所采取的方法。
本文的工作将提出了一种机制，将零信任思想扩展到生产云环境，并从一个升降换挡（lift-and-shift）网络逐步演化到一个完全基于身份的零信任环境。

➤ 云环境中身份管理

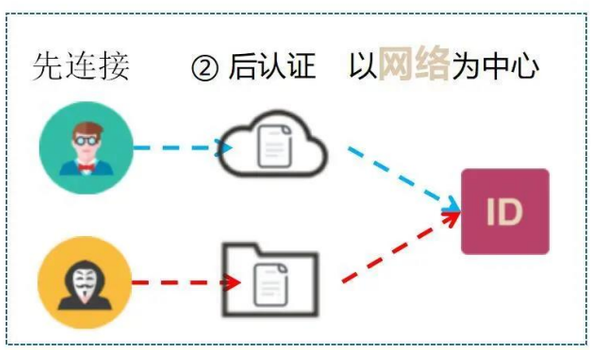
N. Selvanathan, D. Jayakody, and V. Damjanovic-Behrendt. 2019. Federated Identity Management and Interoperability for Heterogeneous Cloud Platform Ecosystems. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES '19). Association for Computing Machinery, New York, NY, USA, Article 103, 1–7.

B. Zwattendorfer, T. Zefferer and K. Stranacher, 2014. An Overview of Cloud Identity Management-Models. In Proceedings of the 10th International Conf. on Web Information Systems and Technologies (WEBIST), pp. 82-92

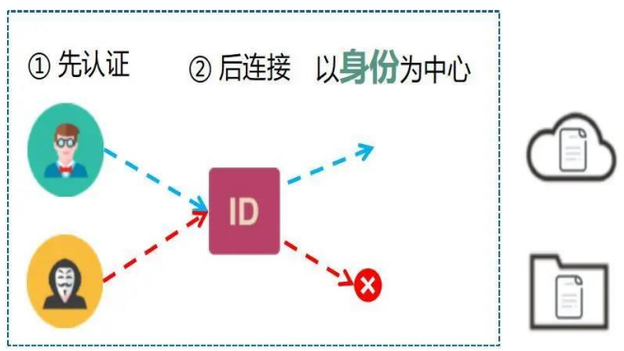
这些文献定义了基于集中身份管理的方法和基于联合的方法。本文的工作也探索了这两个模型如何在现代公共云中发挥作用，并有助于实现云安全边界等安全概念。

WHAT IS ZTA (ZERO TRUST ARCHITECTURE)

零信任是以身份为中心进行动态访问控制，身份的主体可以是人，也可以对设备、系统、应用等。通过定义谁（身份）对哪些资源具有哪种访问权限（角色）来管理访问权限控制，是各类IT系统必不可少的基础安全管理机制和复杂云服务核心的基础安全框架，是对资源提供可控安全的访问解决方案。



传统架构



零信任架构

传统的安全是以网络区域为边界，通过防火墙、VPN、IDS/IPS等网络安全设备建立企业的网络防护边界；一切安全是基于网络位置构筑的信任体系，认为网络内部的人员与设备是可信的。

零信任不同于传统的网络边界安全信任体系，是一套全新的安全理念和安全战略，强调“永不信任，始终验证”，遵循ABCDE原则

- **最小授权：**从零开始，只有认证并授权后才可用，并且认证和授权是需要随时随地进行动态检查验证的，并遵循最小授权原则
- **身份认证与安全策略：**不再仅仅针对网络区域和人员，在而是根据当前环境和状态，对人、时间、地点、设备、系统、应用等的各种属性进行验证确权（最小原则），极大的提高了安全性
- **防范和保护并重：**不再是被动的防堵，因为防不胜防，堵不胜堵，而是被动防堵与主动保护并重，不仅可以做到防患于未然，并且可以做到主动保护（如加密、SDP、MTD等）
- **持续动态：**智能化、动态变化和自适应
- **达到CIA：**可使用、看不见、拿不走、可追溯、能销毁；覆盖云管端、动（传输）静（存储）用（计算处理使用）和前（事前防范、）中（事中阻断）后（事后追溯）

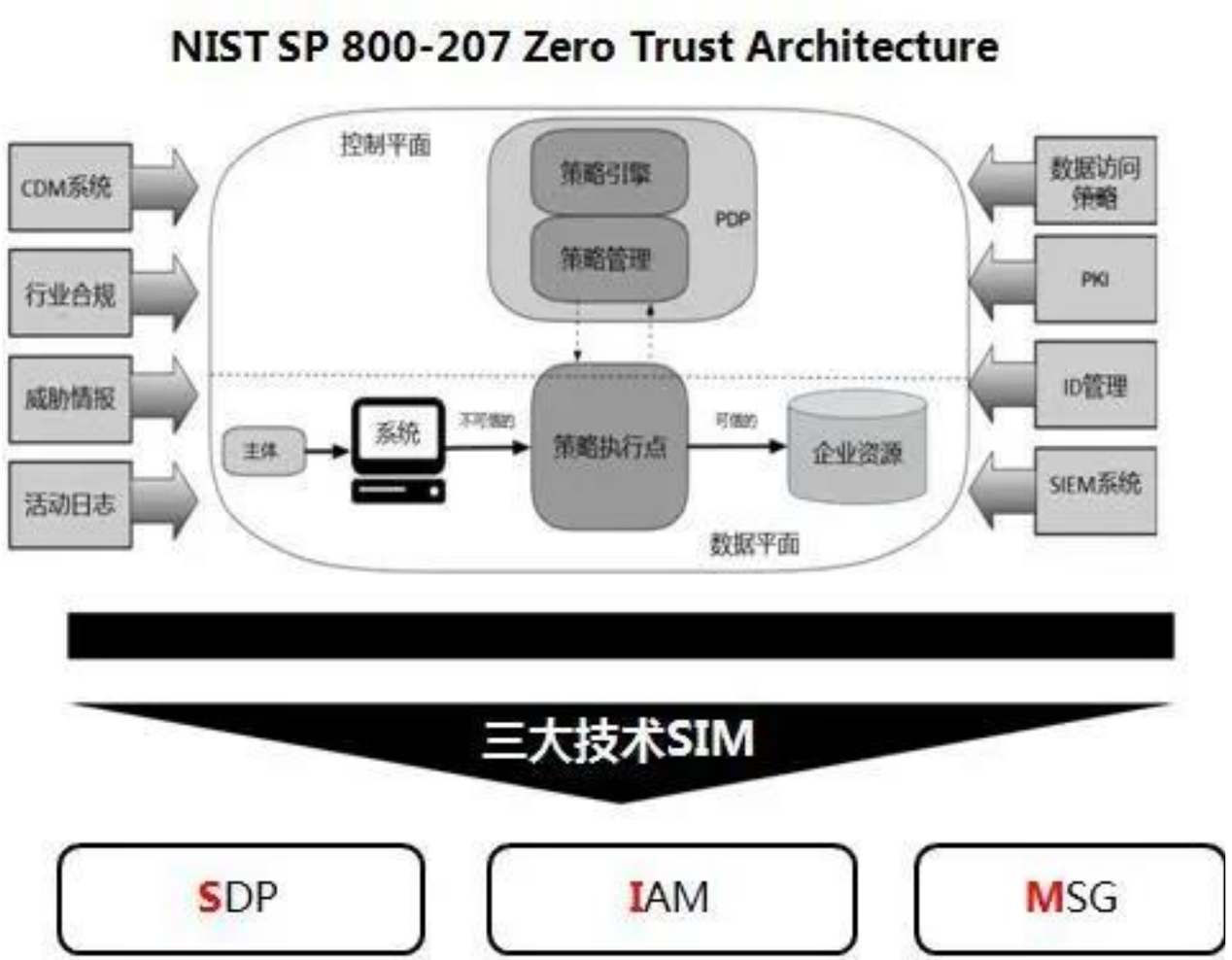
Ref:

http://casgcr.trial.ly200.net/mobile/news-detail/i-147.html
“2019 Zero Trust Adoption Report,” Cybersecurity Insiders, November 2019.
Larry Ponemon. “The state of endpoint security risk: it’s skyrocketing,” Ponemon Sullivan Privacy Report, May 2020.
“2020 Data Breach Investigations Report,” Verizon, May 2020.
“Global Threat Landscape Report,” FortiGuard Labs, August 2020.

ZERO TRUST ARCHITECTURE

目前，零信任有一个标准（美国国家技术标准局NIST制定的ZTA）和3种在业界具有重要影响力的技术SIM（SDP、ZT–IAM、MSG）以及一些其它技术：

- NIST 制定的零信任架构标准ZTA
- CSA制定的软件定义边界SDP技术
- 零信任增强型现代身份管理体系ZT-IAM技术
- 微隔离MSG技术

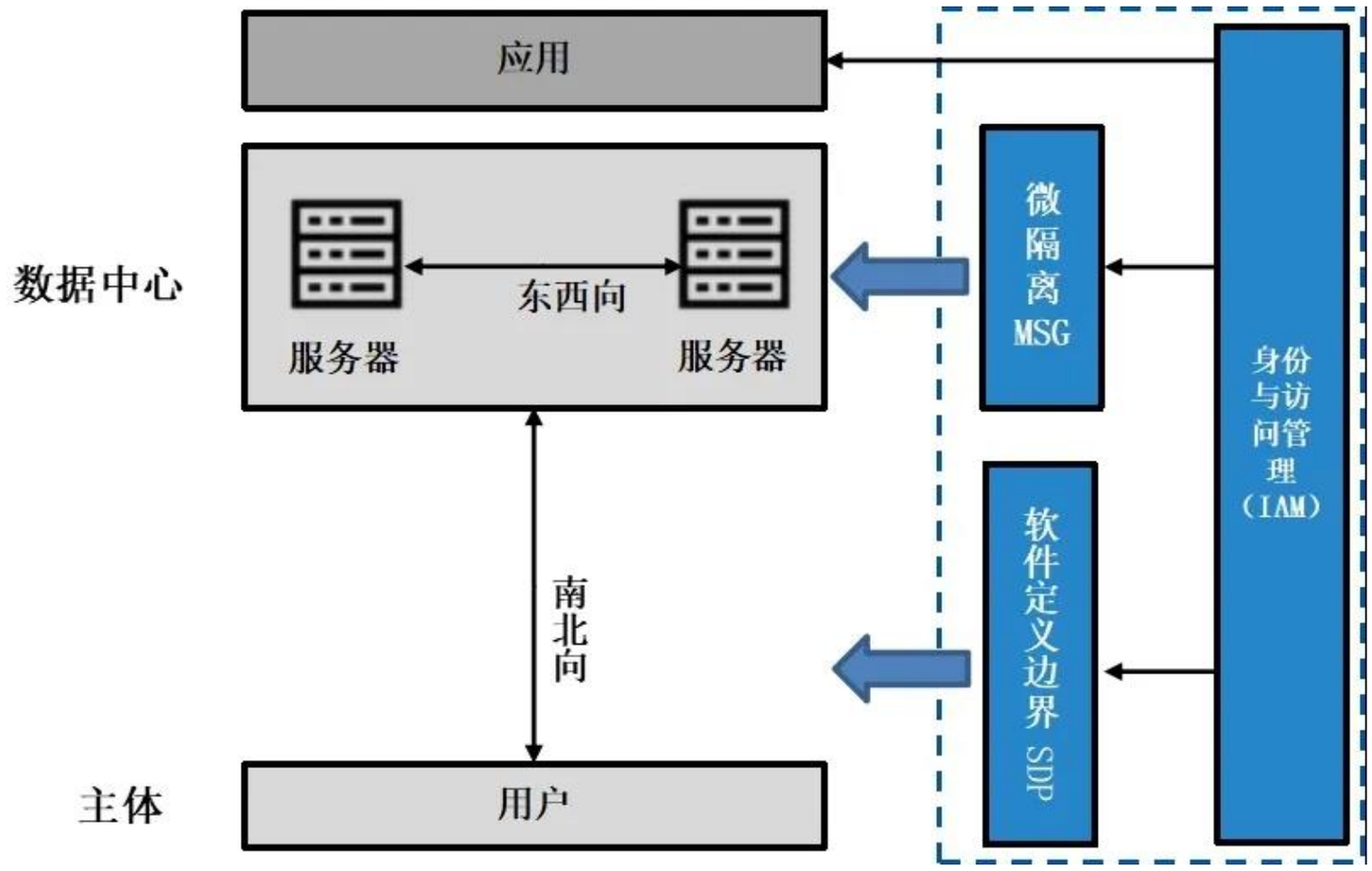


零信任架构（ZTA）设计的7个原则：

- 所有数据源和计算服务都被视为资源
- 无论网络位置如何，所有通信必须是安全的
- 对企业资源的访问授权是基于每个连接的
- 对资源的访问由动态策略（包括客户端身份、应用和被请求资产等的可观测状态）决定，并可能包括其他行为属性
- 企业确保其掌握和关联的所有设备都处于尽可能的最安全状态，并监控资产以确保它们保持在尽可能的最安全状态
- 在访问被允许之前，所有资源访问的身份验证和授权是动态的和严格强制实施的
- 企业收集尽可能多关于网络基础设施当前状态的信息，并用于改善其安全姿态

“SIM”（SDP，IAM， MSG）

2019年,美国国家标准委员会NIST对外正式发布了《零信任架构ZTA》白皮书,强调了零信任的安全理念,并介绍了实现零信任架构的三大技术“SIM”（SDP，IAM， MSG）：



- **南北向流量：**指用户到服务器的流量（Client-To-Server），通常由SDP（软件定义边界）技术来实现南北向零信任安全
- **东西向流量：**指服务器到服务器的流量（Server-To-Server），通常由MSG（微隔离）技术来实现东西向零信任安全
- **身份安全：** IAM作为用户身份信息的输入，实现身份验证以及应用内用户权限的管理

Three models

INTRODUCTION

云计算已经将传统的以网络为中心的安全方法推向了极限。设备、计算类型、SaaS/PaaS服务和公共云的激增挑战了传统的安全概念，并为零信任等新模式打开了大门。

零信任是一个宽泛的术语，它包含了一组相关的概念，即应用程序不应该信任网络，应该对访问其数据的所有尝试进行身份验证。

本文探讨了三种保护云应用程序数据平面的方法，以防止对应用程序及其数据的未经授权的访问，并防止有害的数据泄露。

通过对各种具体安全架构的探索，作者将重点放在以下几个方面：

- 云安全边界（Cloud Security Perimeters），为云中的数据和基础设施提供边界，为敏感信息的不当访问和泄露提供一道防线；
- 云着陆点（Cloud Landing Points），为您的云应用程序的各个部分和本地应用程序之间提供一个安全的集成点，以便通过它进行通信；
- 基于纵深防御和最低权限访问原则的零信任安全架构（Zero Trust security architectures）

论文探讨了保护云应用数据平面安全的各种架构，并探讨了如何从传统的内部网络安全架构过渡到云安全架构，以及如何将它们与兼容零信任安全原则的架构相结合。

CONCEPTUAL MODEL

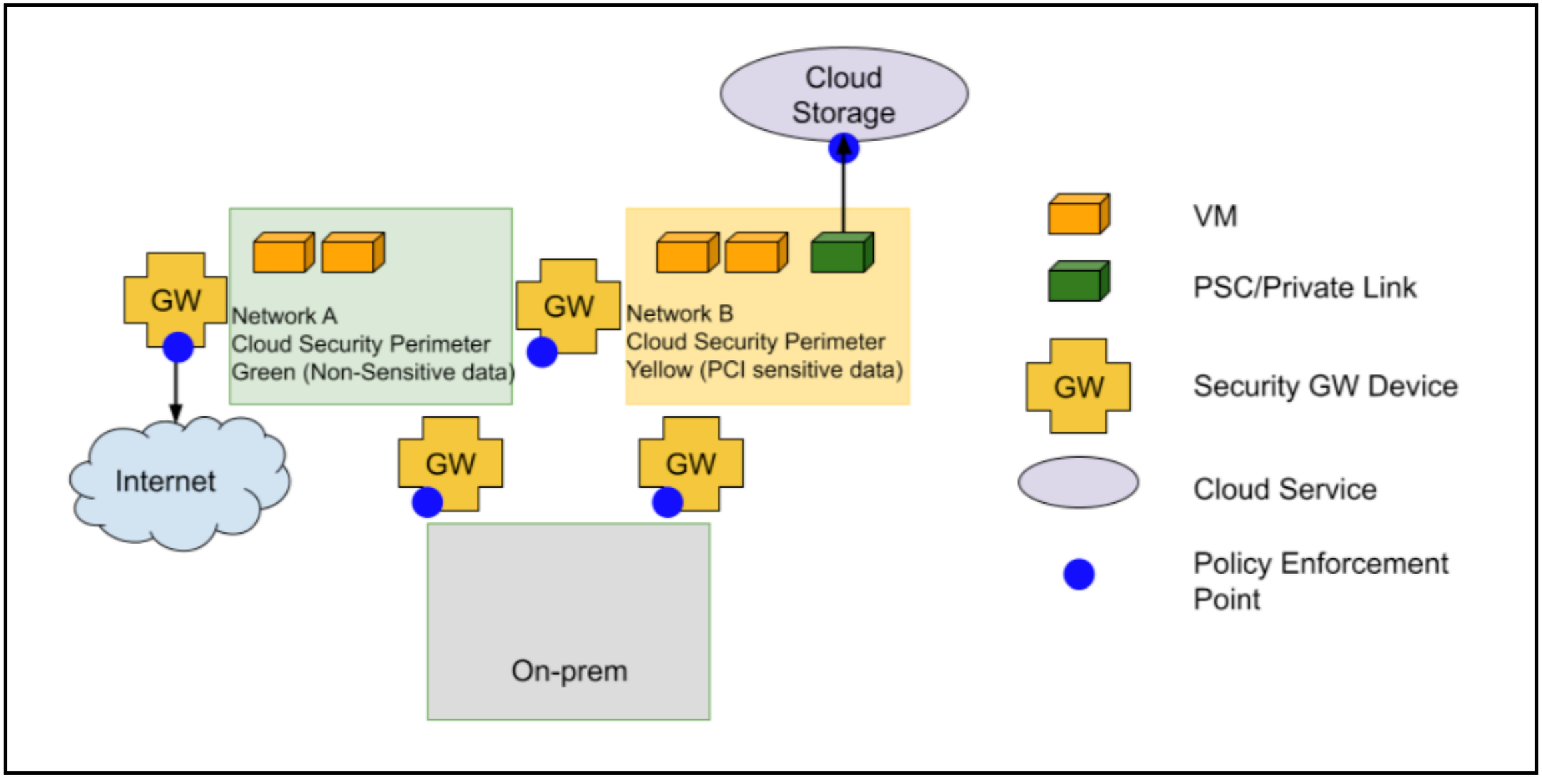
在论文中，作者假设对手相对复杂，有三个优先级很高的目标，因此我们试图防御:

- 防止未经授权的访问——控制和限制应用程序、基础设施和工作负载中的访问和操作特权
- 防止泄漏——客户端人员或客户端应用程序被授权访问给定范围内的数据
- 防止横向移动——当应用程序中被攻破时，限制入侵者移动到其他应用程序或工作负载的能力

由此建立一个安全模型，用于在安全背景下思考云架构。我们将假设应用程序和工作负载由可保护的服务集组成。然后，我们将利用这个概念模型来定义各种体系结构，以实现上述安全目标。当这样做时，我们将看到:

- 应用程序内的通信——当应用程序内的服务相互通信时，保护数据是很重要的
- 应用程序入站通信——当从互联网、内部设施或托管在同一或其他云平台上的服务访问时，提供对应用程序的服务、其数据和云提供商管理的服务的安全细粒度访问是很重要的
- 应用程序出站通信——当应用程序可以连接到基于互联网的服务、本地服务或托管在同一或其他云平台上的服务时，过滤和保护应用程序的数据是很重要的

LIFT-AND-SHIFT ARCHITECTURE



LIFT-AND-SHIFT ARCHITECTURE — CHALLENGES

定义身份->身份管理->访问控制

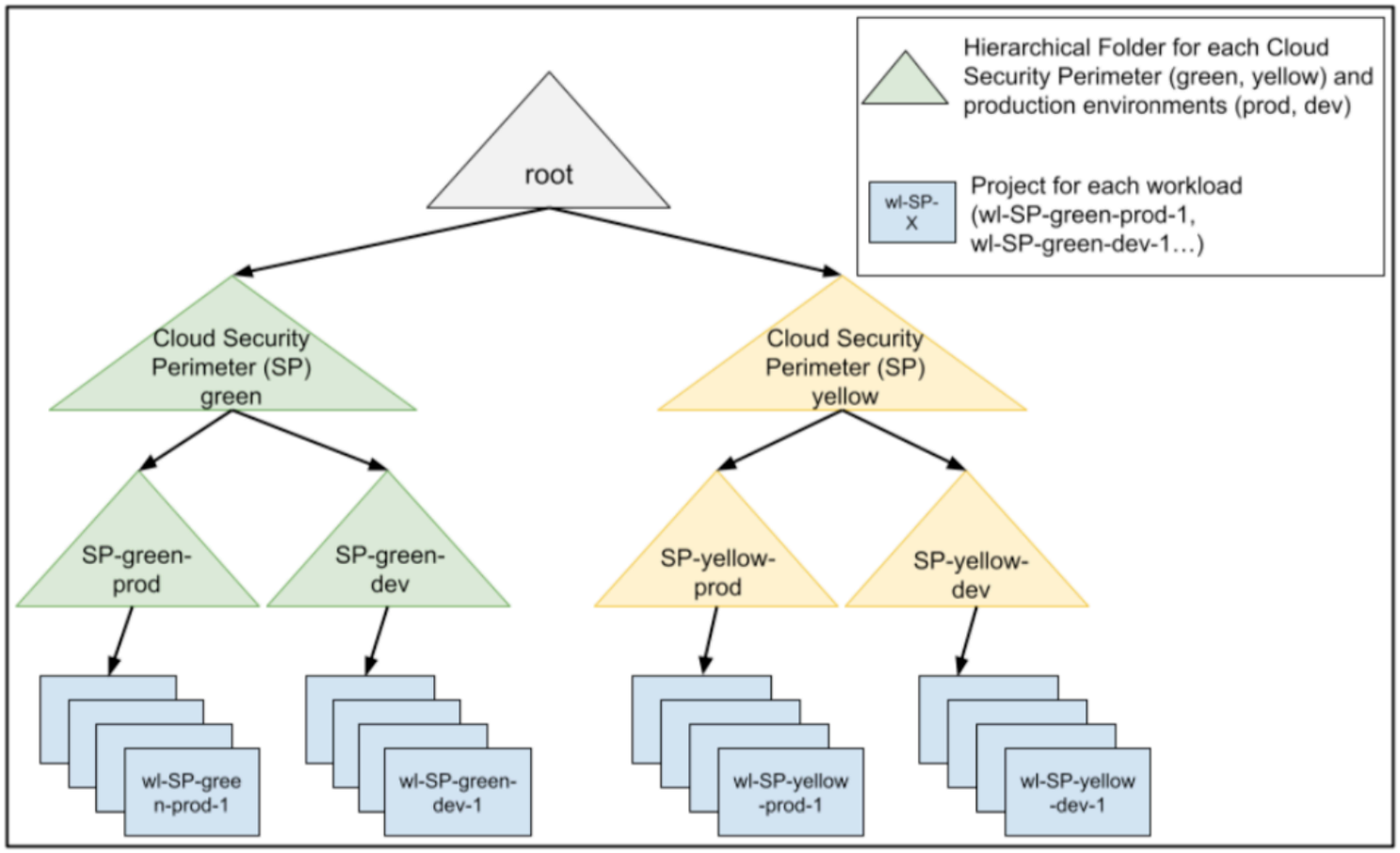
云管理服务(Cloud Managed Services) 本质上是云原生的，它的引入和使用使身份识别和网络网络的提升和转换架构原则变得复杂，如下所示:

- 身份——将应用程序的遗留身份与新引入的云基础设施身份分离的方法经常用于此架构。当使用使用本地云平台标识的云管理服务时，这种方法不再可行。这使得遗留应用程序和云管理服务很难对彼此进行身份验证和授权。

- 网络——同样，云管理服务的网络访问路径由云平台提供商实现和控制。路由通常在应用程序级进行，云提供商管理底层网络基础设施，从而创建使用传统的内部网络方法控制访问的挑战。

For more details, please turn to the Paper page 11-12.

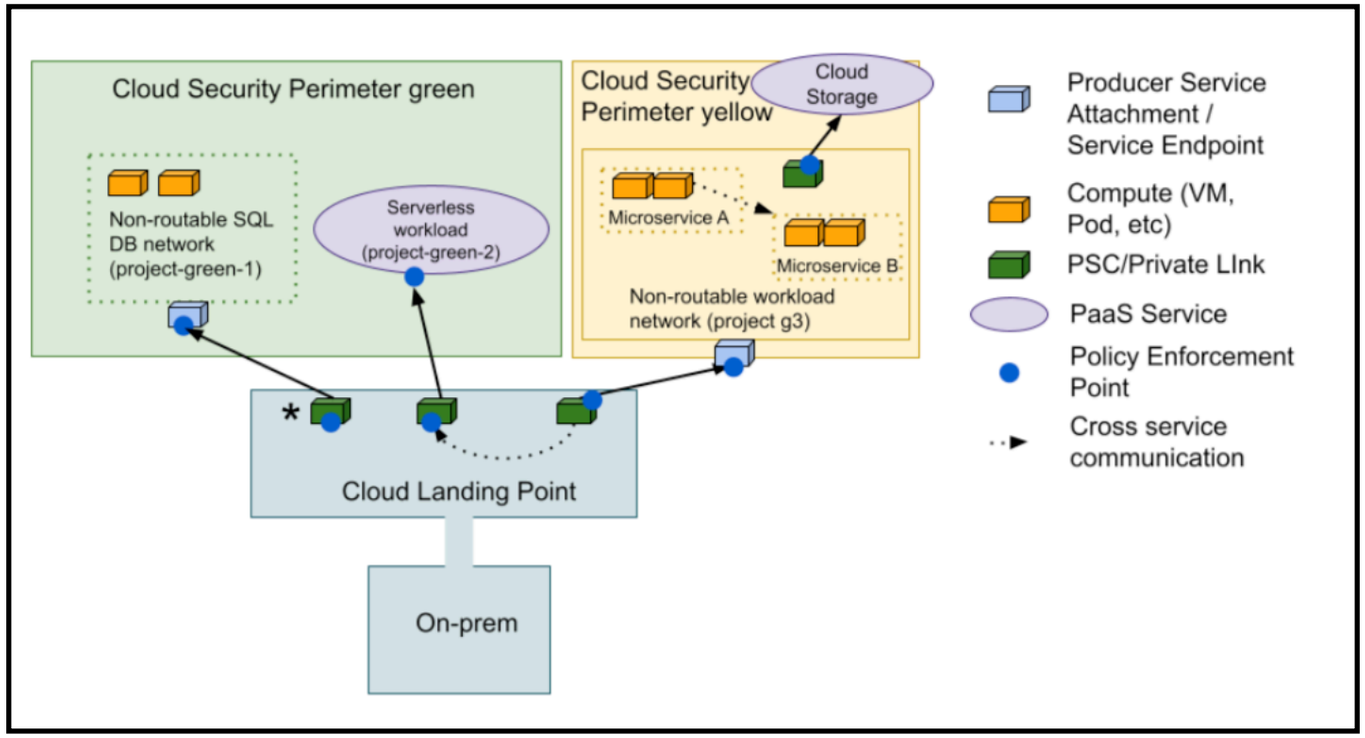
HYBRID SERVICES ARCHITECTURE



Best practices :

- 项目和网络隔离
- VPC SC
- 层次结构的使用
- 依赖管理
- 分层防火墙
- 标签
- 组织策略

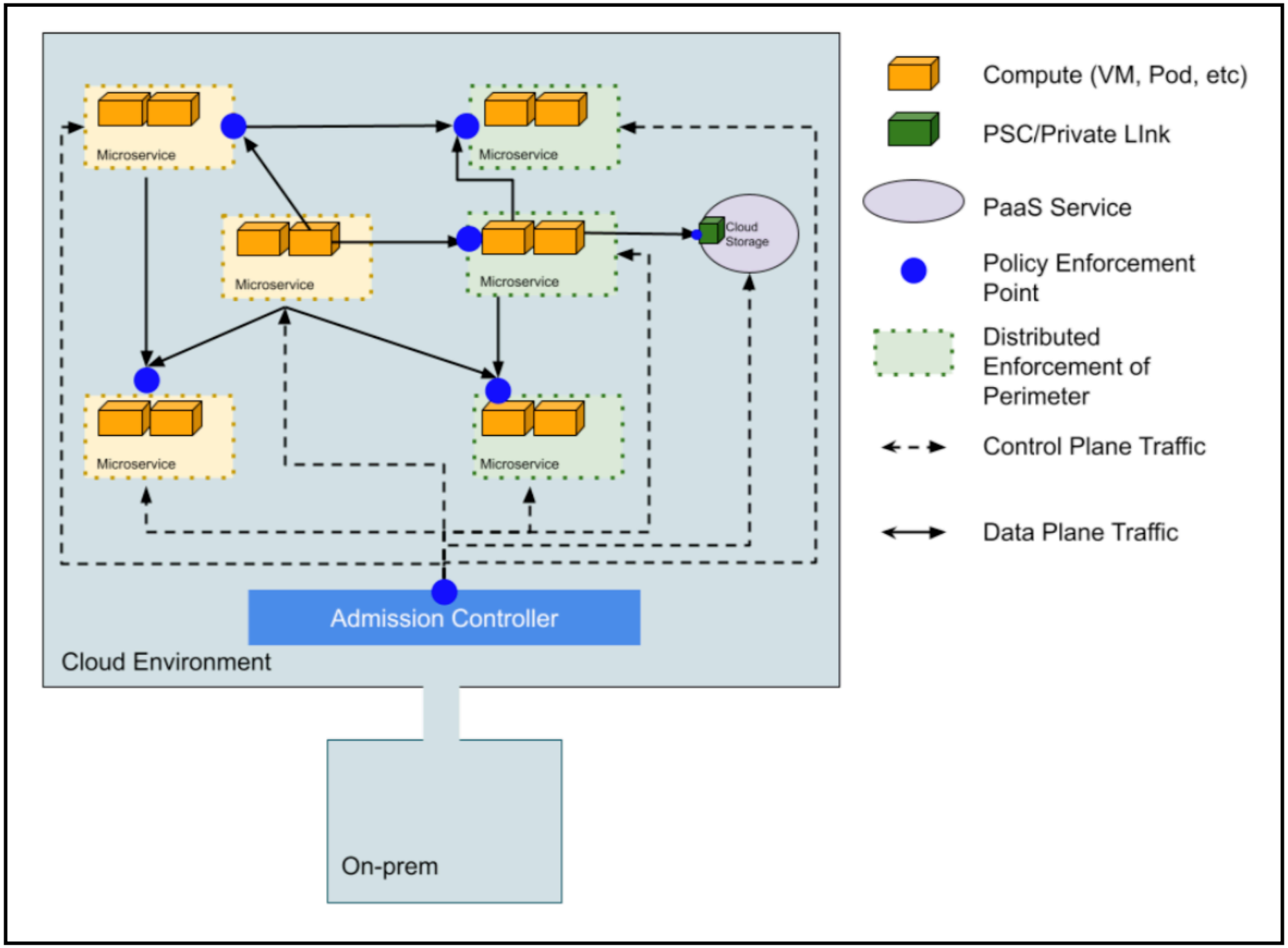
HYBRID SERVICES ARCHITECTURE



构建云着陆点网络架构有三个主要目的:

- 在云环境中创建beachhead ，从概念上讲，它是内部基础设施的扩展，可以在其中公开工作负载
- 将基础设施网络问题(如互连的对等连接位置)与云本地应用程序和服务架构问题解耦
- 使计算非均质性

ZERO TRUST DISTRIBUTED ARCHITECTURE



ZERO TRUST DISTRIBUTED ARCHITECTURE

该模型由多个元素组成：

- 具有上下文属性的应用层策略

  ——通常每个服务都有一个标识

- 分布式强制边界

  ——分布式强制边界指的是应用于微服务粒度的零信任策略的概念，它在作为此类微服务一部分的计算后端组周围创建一个逻辑安全边界

- 一组服务的逻辑范围

  ——Zero Trust模型为定义每个服务控件提供了很大的粒度，但在管理数百或数千个服务时，这有复杂性的权衡

ZERO TRUST DISTRIBUTED ARCHITECTURE

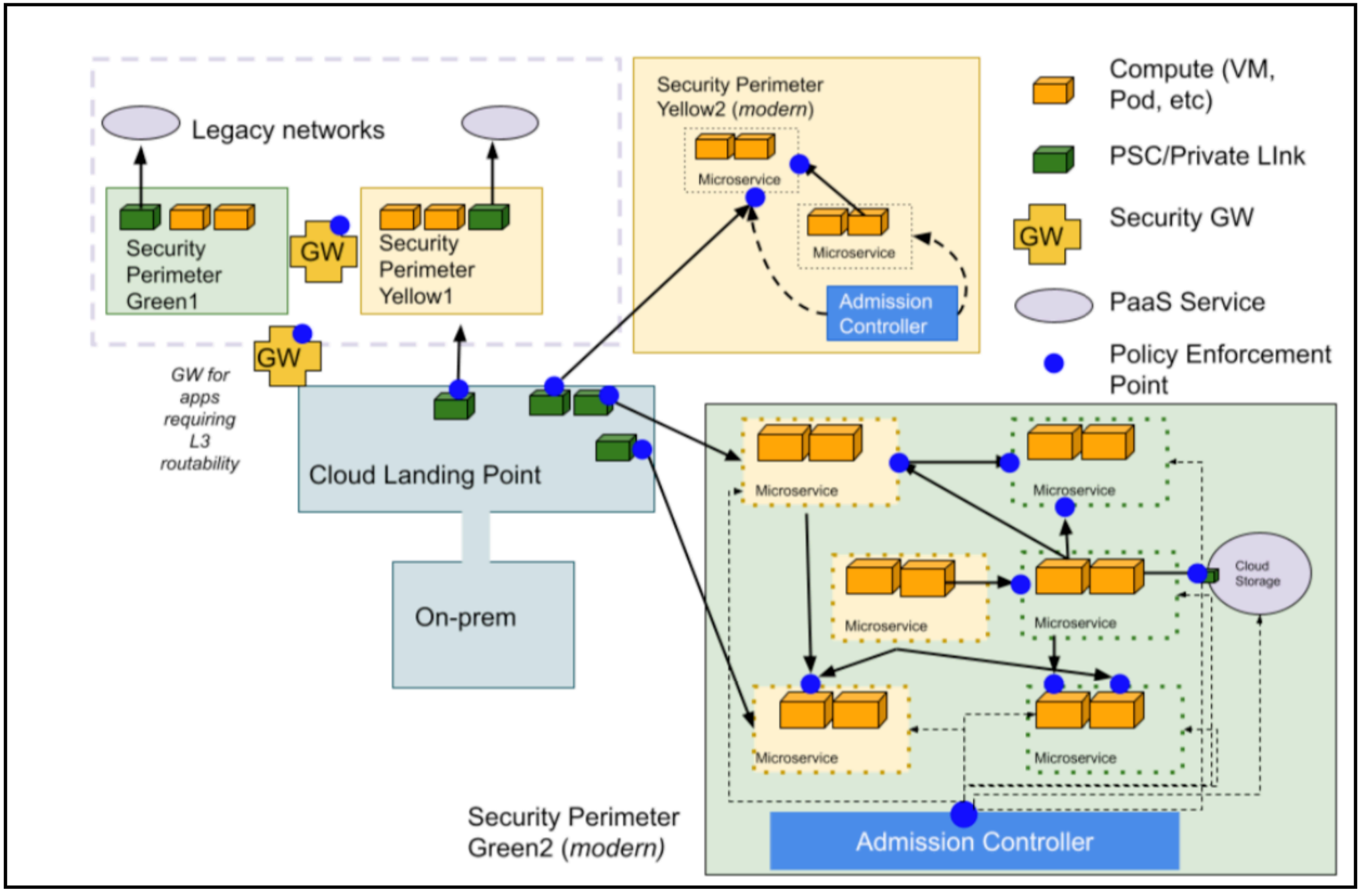
此外，这种方法成功的一个关键因素是确保在网络上运行的代码的来源(因为该代码本身负责执行策略)。这通常通过结合两个条件来实现:

- 将DevOps限制在特殊情况下，并严格审核此类情况
  （Limit DevOps to exceptional break-glass cases for access to production, and closely audit such access. ）
- 软件供应链和二进制授权的强制管理
  （Robust governance of the software supply chain and binary authorization ）

虽然这些控件的细节不是本文的重点，但值得注意的是，它们的组合创建了一个信任链，使安全策略的分布式强制变得可行和有效。这两种控制在实践中都很难实现，但如果能够实现它们，就可以创建一个非常强大的环境，用于部署高度扩展的工作负载。

对于许多企业来说，将Zero Trust体系结构组合到前面考虑过的体系结构中可能更为现实

COMBINED APPROACHES



THANKS